

Decálogo de protección de datos para el personal sanitario y administrativo

1. Trata los datos de los pacientes como querrías que tratarasen los tuyos.
2. ¿Estás seguro de que tienes que acceder a esa historia clínica? Piénsalo. Solo debes acceder si es necesario para los fines de tu trabajo.
3. Recuerda: tus accesos a la documentación clínica quedan registrados en el sistema. Se sabe en qué momento y a qué información has accedido. Los accesos son auditados posteriormente.
4. Evita informar a terceros sobre la salud de tus pacientes, salvo que estos lo hayan consentido o tengas una justificación lícita.
5. Cuando salgas del despacho, asegúrate de cerrar la sesión abierta en tu ordenador. No facilites a nadie tu clave y contraseña; si necesitas un acceso urgente, contacta con el departamento de informática.
6. No envíes información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si fuera imprescindible, no olvides cifrar los datos.
7. No tires documentos con datos personales a la papelera; destrúyelos tú mismo o sigue el procedimiento implantado en tu centro.
8. Cuando termines de pasar consulta, cierra con llave los armarios o archivadores que contengan documentación clínica.
9. No dejes las historias clínicas a la vista sin supervisión.
10. No crees por tu propia cuenta ficheros con datos personales de pacientes; consulta siempre antes con el departamento de informática.